



K-12 Wireless Networks

A Planning Guide for K-12 IT Professionals

November 2010

THIS WHITE PAPER IS FOR INFORMATIONAL PURPOSES ONLY, AND MAY CONTAIN TYPOGRAPHICAL ERRORS AND TECHNICAL INACCURACIES. THE CONTENT IS PROVIDED AS IS, WITHOUT EXPRESS OR IMPLIED WARRANTIES OF ANY KIND.

© 2010 Dell Inc. All rights reserved. Reproduction of this material in any manner whatsoever without the express written permission of Dell Inc. is strictly forbidden. For more information, contact Dell.

Dell, the DELL logo, and the DELL badge, Dell™ PowerConnect™ W-Series, are trademarks of Dell Inc. Microsoft® Windows® are either trademarks or registered trademarks of Microsoft Corporation in the United States and/or other countries. AirWave®, AirWave Wireless Management Suite™ (AWMS), Aruba Networks®, Aruba Mobility Management System® are trademarks of Aruba Networks, Inc.

Note: All scaling metrics outlined in this document are maximum supported values. The scale may vary depending upon the deployment scenario and features enabled.

Other trademarks and trade names may be used in this document to refer to either the entities claiming the marks and names or their products. Dell Inc. disclaims any proprietary interest in trademarks and trade names other than its own.

Contents

<i>Introduction</i>	4
Scope	4
<i>Planning Wireless Connectivity</i>	5
Scalability	5
Data, Voice and Multimedia Access	6
Mobility	6
Security	6
Reliability	7
Management	7
Cost	7
<i>Enabling today's learning environments with the latest in WLAN technology</i>	8
<i>Introducing PowerConnect-W Components</i>	10
PowerConnect W-Series Access Points	10
PowerConnect W-600 Series	10
PowerConnect W-3000 Series	11
Airwave Management Wireless Suite for PowerConnect W-Series products	11
Modules for PowerConnect W-Series Controllers	11
<i>K-12 Wireless Network Topology</i>	12
Data Center or Equivalent	12
School Buildings	12
Outdoor Areas	13
Remote Users and Temporary Teaching Environments	13
Virtual Intranet Agent	13
<i>Multivendor Wired and Wireless Management</i>	13
Applications and services running on backend	14
<i>More Efficient School Networks with Adaptive Radio Management</i>	14
<i>Realizing the full potential of your K-12 Network</i>	15
Scalability	15
Mobility	15
Data, Voice and Multimedia Access	15
Security	16
Reliability	16
Management	16
Cost	17
<i>Conclusion</i>	17

Introduction

The increased use of wireless devices in K-12 schools has created a unique opportunity to dramatically improve student engagement and mobility of the teaching environment within a school campus. The integration of audio, video and graphics animation, coupled with interactivity, has enabled new teaching paradigms that expand the learning opportunities for all students. In addition, the Internet and other communications networks have opened access to a plethora of information never before available, taking students well beyond traditional classroom resources.

Dell's Connected Learning Strategy¹ addresses this shift in the K-12 environment. The Connected Classroom² from Dell embraces the idea of learning environments that engage students using innovative education technology and the various ways those practices are realized in the classroom. Here, students can develop critical thinking skills, express themselves creatively, and communicate and collaborate more effectively. Dell Connected Classroom supports a wide range of devices that allow pupils to connect, collaborate and learn. It helps teachers personalize learning by offering different instruction techniques according to the individual learning styles of the pupils. With student response systems and software, teachers can determine immediately if students understand the subject matter. Teachers in a Dell Connected Classroom can view all student devices simultaneously in an adjustable thumbnail size. Students can work on the interactive whiteboard while teachers concurrently capture notes from peer discussions and share them with the students for review.

Supporting the Connected Classroom is the Dell Connected Infrastructure³, which offers a range of products and services based on open standards that can easily be integrated into existing school computing environments to facilitate information sharing and collaboration—securely and effectively. There are key technology implications that enable the progression to online, virtual or blended learning environments. Access to information is the common goal regardless of pedagogy, and one of the key components in the Connected Infrastructure is K-12 Networking. Contemporary teaching environments rely on network connectivity, which when used in conjunction with an effective wireless access infrastructure, can enable secure, mobile learning with a price tag that allows for ubiquitous deployment.

Scope

K-12 IT leaders must address a number of critical planning considerations as schools undertake student-computing initiatives that ensure students and teachers have fast, secure and reliable network access to the digital tools and content. This paper explores guidelines to consider when implementing wireless networks so that you can effectively support connectivity for your students, teachers and staff. It also

1 To learn more about the Dell's Connected Learning strategy –

http://www.dell.com/content/topics/topic.aspx/global/segments/topics/k12/us/dell_learning_ecosystem?c=us

2 To learn more about the Dell's Connected Classroom – <http://content.dell.com/us/en/K12/connected-classroom-main.aspx?c=us>

3 To learn more about the Dell's Connected Infrastructure – <http://www.dell.com/connectedinfrastructure>

illustrates the benefits of Dell's PowerConnect W-series as part of a networking solution for K-12 environments.

Planning Wireless Connectivity

Building a connected learning environment helps schools transform education for the digital age. By providing the right technology needed to connect each member of the school system together, schools can quickly impact the relevance of their teaching and learning environments as teachers enable the development of 21st Century skills to the next generation of digital workers. Connectivity and mobility of classroom devices, like laptops and tablets (Connected Classroom), rely on wireless connectivity (Connected Infrastructure). Connectivity also extends to the inclusion of parents, the local and global community to build career and college ready students (Connected Community).



As you plan your connected learning strategy there are a number of factors to consider for the wireless networking environment:

Scalability

Scaling a network infrastructure to meet growth is a challenge for small and large K-12 schools. In schools that allow students to bring in their own computers, there is a paradigm shift in the makeup of devices that come into the classroom. Mobile devices now include not just laptops, but also eTextbooks, student response systems, tablets and smart phones. These devices are battling for the limited number of network connections. To make matters worse, these devices will often attempt to connect simultaneously. For example, when the school bell rings in the morning and classes are in session, there will be an increased demand as many students are connecting all at once. Then the bell rings for lunch, and the network demand drops

immediately. K-12 networks need to be able to scale over the long-term and also need to handle the ups and downs of network demand on a daily basis. Networks in most schools are unable to satisfy today's connectivity requirements. Many classrooms cannot even accommodate a mobile cart—a shared installation of networked laptops for a special lesson or activity. Adding computer labs and PC-equipped work areas requires intrusive infrastructure installations and expensive upgrades.

This growing demand for scalable access to digital learning environments can be addressed by adding a Wireless Local Area Network (WLAN) which liberates students, teachers and administrators from the hard-wired network, thereby increasing use of digital devices for teaching, making possible new digital content, collaborative learning and providing ubiquitous access to network-based resources.

Data, Voice and Multimedia Access

This new mix of devices has coincided with the advent of new multi-media, interactive teaching, and learning applications. The result is a requirement for a new class of network that is multimedia-grade. Network connectivity needs to offer sufficient bandwidth and quality of service intelligence to reliably deliver the intended data, voice, and video applications over the air to all students, simultaneously, even in densely populated classrooms.

Mobility

The desire to make the best use of classrooms, libraries, labs and common areas around the school has increased the need for portable devices with mobile network connections that can be used wherever and whenever needed. Students should be able to roam using their laptops from classrooms to hallways and even outdoors without being disconnected nor signing on again. Students today are on a technology and information learning curve that is continuing to accelerate and they will increasingly use their capacity to learn outside the school environment. Technology will become more mobile, ubiquitous, less expensive, and more interconnected. The wired computer lab as we knew it has disappeared in favor of collaborative spaces.

The WLAN is also being used more frequently for voice applications, requiring seamless roaming across a school campus.

Security

Schools have extensive network and user security requirements, many of which are unique to schools. Wireless networks introduce special concerns and considerations including who is allowed onto the network, controlling where they can go, and preventing intruders.

To protect its networks and accommodate its varied constituents, schools need tight control over who is allowed onto the wireless network. Nearly all WLAN solutions provide one or more levels of encryption and authentication. However, most require client software on every computer and device. This additional work can paralyze a limited IT staff, especially given the mix of older computers and operating systems often found in schools.

Add to this that increasingly, students are bringing their own devices with varying degrees of security protection and expecting to connect to a wireless network.

The applications used in the classrooms are typically licensed only to authorized users, and reasonable care must be taken to enforce this condition of use.

Unauthorized traffic will consume bandwidth, sometime purposefully, degrading application performance and interfering with the work of legitimate network users.

Reliability

Reliability of any educational network is paramount. To be the foundation of a connected learning environment, educational networks must be available at all times. When a network has a reliability problem, students and teachers are disconnected. Learning is disrupted. Students and teachers are frustrated. Planned lessons that rely on digital content or may have to revert back to lectures. Student and teacher performance suffers.

The wireless network must be able to maintain high availability, even when confronted with sources of interference, whether that source of interference is a neighboring public Wi-Fi hotspot, or a non-Wi-Fi device such as a microwave or wireless camera.

Management

Mobile devices require a new approach to management that is more flexible to address a user community that can now connect anywhere. The network must also be simple to manage and easily integrate with helpdesk functions. This is particularly important since schools typically have limited IT personnel, with staff often pulling double-duty. For example, a computer instructor might also serve as on-site network administrator.

The K-12 wireless network is a mission-critical IT service. Thus, the management of the wireless network is extremely important. Downtime has a real effect on the teaching and learning, so K-12 needs to fix problem spots proactively and use historical data to make the right decisions. It's important to note that many schools are seeing the WLAN becoming the platform of choice for students, whether or not they planned for it. Schools that aren't monitoring their facilities for rogue Access Points (APs) are creating large security risks.

The ability to manage and update the devices and applications such as handhelds, Voice over WLAN (VoWLAN), Video or printers attached to the wireless network is also essential.

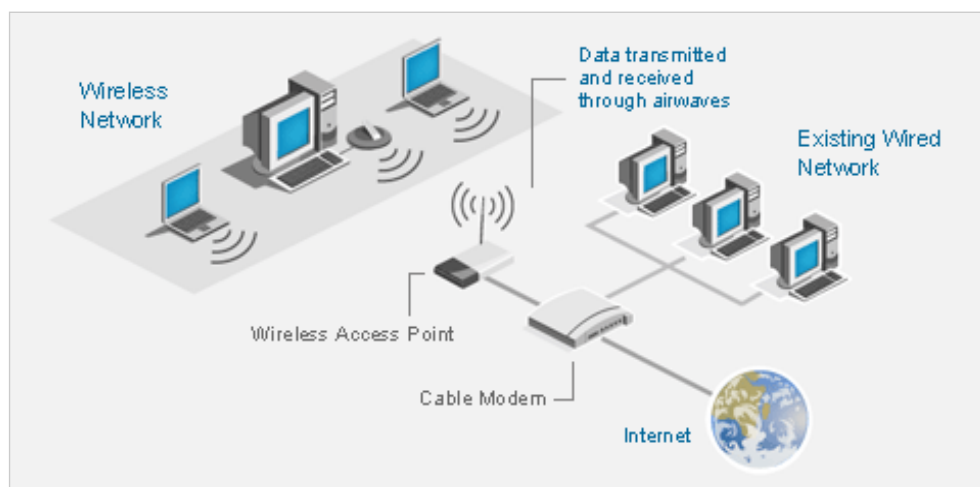
Cost

Schools, particularly public schools, face greater financial pressures than most enterprises. There is an enormous need to use every dollar efficiently and effectively, and to ensure that capital purchases have a long, productive life. This financial pressure requires that WLAN deployment costs be kept low, that the existing infrastructure be leveraged, and that the investment protected for years to come.

K-12 IT decision makers need to evaluate all key components required to deploy a successful, secure, manageable and scalable WLAN infrastructure that's affordable. In short, provide less well and plan for future scalability.

Enabling today's learning environments with the latest in WLAN technology

A WLAN links computing devices using some wireless distribution method, and provides a connection through an access point to internal resources and to the wider Internet. This gives users the ability to move around within a local coverage area and still be connected to the network. The diagram below illustrates a typical wireless networking implementation.



One of the most recent wireless standards to emerge is 802.11n. It's faster, less prone to interference, has improved security and is ready to handle the multimedia requirements of digital learning environments. 802.11n is an enabling technology that accelerates the shift from wired to wireless as the preferred access method in classrooms and across districts. With the introduction of 802.11n, K-12 schools can now deploy wireless networks with:

Increasing capacity and performance. Allow your students and teachers to use rich multimedia content with fast access. 802.11n enables increased data rates, improving the usable data capacity of an access point from perhaps 15-20 Mbps with 802.11a/g to 150-300 Mbps.

Comparison of different 802.11 transfer rates (source: Intel Labs)

IEEE WLAN Standard	Over-the-Air (OTA) Estimates	Media Access Control Layer, Service Access Point (MAC SAP) Estimates
802.11b	11 Mbps	5 Mbps
802.11g	54 Mbps	25 Mbps (when .11b is not present)
802.11a	54 Mbps	25 Mbps
802.11n	300 Mbps	150 Mbps

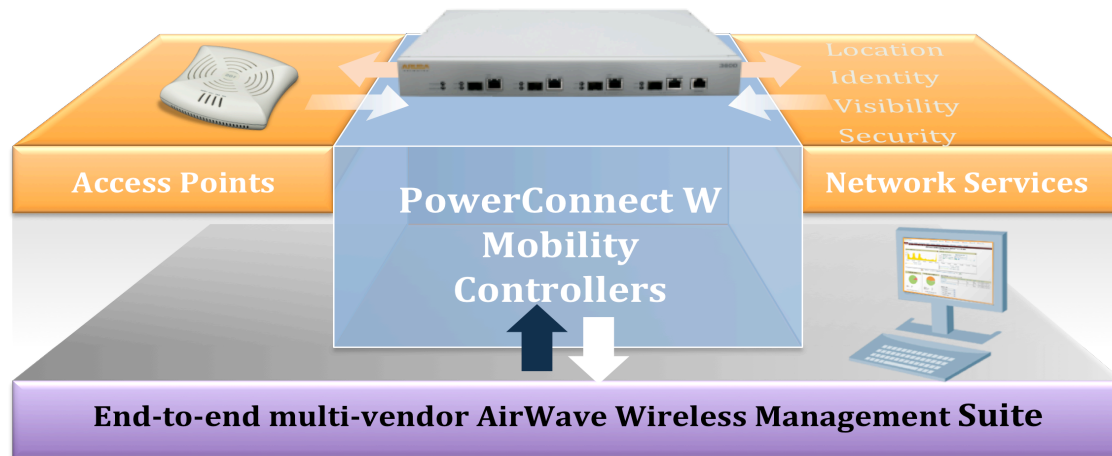
Improved range. Use the entire school as your mobile learning environment. An 802.11g connection from AP to client can usefully extend up to 60 meters in open, unobstructed areas but this range drops to only 20 meters in office environments. 802.11n increases this through multiple-input, multiple-output (MIMO) techniques, which involve driving multiple antennas on the access point and the client. The use of MIMO improves the connection data rate for a given range, and somewhat extends the range at the edge of a cell, useful if a network is designed for coverage rather than capacity.

More uniform 'reliable' coverage. Make sure your learners can connect for anywhere anytime learning. Coverage in Wi-Fi networks can be spotty. A user may have a good signal in one location, but moving the client a short distance, stepping in front of it, or even opening a door across the room can affect the received signal strength, moving the client into a coverage 'null' and reducing performance. One contributor to this issue is multipath propagation, and the best technology to counter this to date has been antenna diversity – nearly every Wi-Fi device sports two antennas, and switches between them because when one is in a multipath null, the other should still have a workable signal. The MIMO technology in 802.11n is extremely effective in reducing the effect of multipath nulls by allowing antennas to work together to recover the original signal: the effect is that the incidence and severity of signal nulls is greatly reduced, especially as a mobile device moves across the network.

Lower network costs. The cost of connecting users with a high speed Wi-Fi connection is significantly less than the cost of wiring each device. Not only is the network less expensive to deploy but also the network is also less expensive to power, cool and administer. Cover more of your school with less. In a homogeneous 802.11n network, improved range and more reliable coverage can allow Access Points (APs) can be spaced further apart. This reduces costs in a number of ways: fewer APs, lower installation costs, possibly fewer LAN edge switch ports, and fewer outdoor APs to cover campus areas between buildings. But to date, it has been difficult to realize these gains because of the need to support legacy clients, and because it is usually more important to increase data rates than to extend range (most enterprise WLANs are designed for capacity rather than coverage).

Introducing PowerConnect-W Components

Dell PowerConnect W-Series solutions help customers deploy and manage wireless networking solutions. The Dell PowerConnect-W WLAN components consist of Access Points (AP), Controllers and management suite of products.



PowerConnect W-Series Access Points

Dell PowerConnect W-Series Access Points (APs) are 802.11n indoor access points with features to address the specific performance and productivity needs of distributed networks, from large school districts to schools or just a few Connected Classrooms. Configured by Dell PowerConnect W-Series Controllers, the APs require no manual configuration, utilize automatic software updates and are managed centrally. This saves K-12 network managers time and money. 802.11n Wi-Fi support enables wire-like performance of up to 300Mbps, with single and dual-radio options, 2.4Ghz and 5Ghz band support, 802.11a/b/g/n client access and internal/external antenna options.



PowerConnect W-600 Series

The PowerConnect W-600 Series is ideal for smaller network deployments, offering a balance of features and value while working seamlessly with any mix of PowerConnect W-Series access points. With the W-600 Series and the access points, a wireless solution can be quickly deployed with minimal IT presence or experience. With optional feature modules, the PowerConnect W-600 Series can be further configured to accommodate secure productivity and application delivery needs. The W-651 takes the solution one step further by offering an internal dual-band, single-radio AP, so that small business can expand later with additional W-Series access points. All controllers feature USB ports for print servers and expandable storage needs, thereby delivering a single solution for remote and small office location.



PowerConnect W-3000 Series

The PowerConnect W-3000 Series of Mobility Controllers deliver a high-performance, secure and reliable wireless management and access solution for the enterprise network. Deployed in medium to high density networks typically, the W-3000 Series can be integrated into the backbone and support up to 128 APs, with optional feature modules for further protection and firewall capabilities for the wireless network. A variety of secure options (including authentication, encryption) enable communications with APs, as well as redundancy options to meet IT administrator availability requirements.



Airwave Management Wireless Suite for PowerConnect W-Series products

The Dell PowerConnect W-Series is further enabled with the Airwave Management Wireless Suite (AWMS) powered by PowerConnect-W Networks. AWMS is a comprehensive suite of management options for your PowerConnect W-Series based-network, delivering operational efficiency for rapidly changing and growing networks, while simplifying management of your network. AWMS has an easy-to-use interface to readily support the mobile workforce and configure setups, while IT personnel can quickly expand the network and reduce disparate tools they need to support the network. AWMS offers unique capabilities including a mobile device manager, which monitors and offers a single view of all devices on the network, as well as wired-equipment configuration and reporting.

Modules for PowerConnect W-Series Controllers

The functionality of a school network can be further expanded with add-on modules for PowerConnect W-Series Controllers.

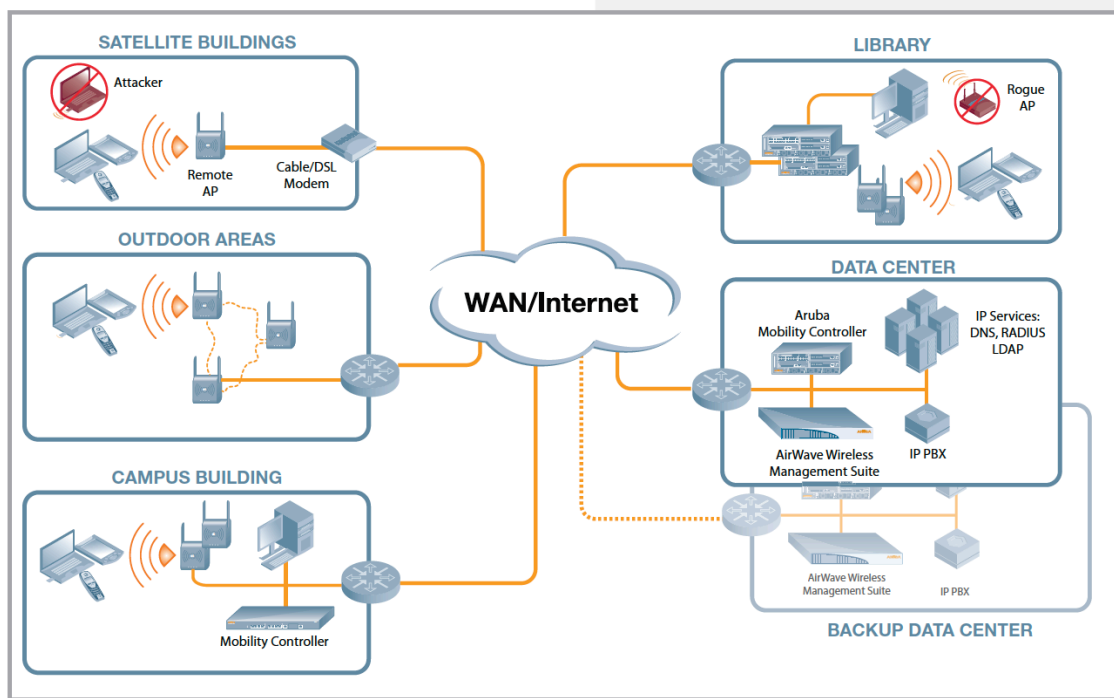
RFProtect Module: RFProtect integrates wireless security into the network infrastructure without requiring a separate system of RF sensors and security appliances and enables government-grade Wireless Intrusion Prevention. RFProtect also includes powerful Spectrum Analyzer capabilities, which provide a critical layer of visibility into non-802.11 sources of RF interference and their effects on 802.11 wireless LAN channel quality. As a result, RFProtect eliminates unwanted wireless threats and interference, while optimizing network performance.

Wireless Intrusion Protection (WIP) Module: Actively protect the network against network threats, while detecting and preventing threats before they affect your network and mobile workforce. The WIP module offers impressive capabilities to detect and disable rogue APs, man-in-the-middle attacks, Denial of Service (DoS) and other threats before they penetrate the wired network.

Policy Enforcement Firewall (PEF) Module: Robust firewall protection and network policy enforcement for your wireless network. The PEF module delivers a unified point of authentication with encryption and policy enforcement, allowing organizations to quickly enforce access policies specifying who can access the network and which areas of the network are accessible. PEF also supports voice over Wi-Fi deployments for the enterprise with SIP protocol support.

K-12 Wireless Network Topology

The diagram below depicts a typical K-12 centralized data center and campus WLAN and WAN environment.



Data Center or Equivalent

Depending on the number of remote locations and total number of APs, one or more master Mobility Controllers are installed in the data center. These controllers can also terminate APs used for wireless connectivity in the data center building and remote APs used in small remote locations and home access applications. A master controller supports local can support up to 500 remote controllers and is the single interface for configuration and management. A master controller can also back up a controller in a remote location in the case of an outage. To scale for larger deployments, multiple master controllers can share the load of managing local controllers and APs in remote sites, and the Airwave Management Wireless Suite (AMWS) can be used as the single interface of management and configuration.

School Buildings

Depending on the number of APs required in each location, a different model of Dell Mobility Controller (called a local controller) is installed. All Dell controller models run the same software and have the same functionality, but differ in AP capacity – from up to 6 to 2,048 APs. Each local controller gets its configuration from the master controller. Application continuity and PCI security levels are enforced at a per-user level by the local controller. Local controllers also offer Wireless Intrusion Protection and can offer provide authentication services and/or pass-through requests to the data center. Each local controller automatically calibrates the RF coverage to optimize application performance and cover any coverage holes. Further, to extend

wireless coverage in areas that are hard or costly to wire, Dell APs can backhaul over Wi-Fi using the award-winning Secure Enterprise Mesh technology.

Outdoor Areas

Most Dell APs can be deployed in covered outdoor areas for use cases such as digital signage, surveillance cameras, blue light call boxes, or just outdoor student network access. For harsh outdoor conditions, ruggedized APs are also available. In cases where the Ethernet network has not been extended to these outdoor locations, any Dell AP can create a mesh connection back to a Dell network-connected AP that has been enabled for mesh. The AP will continue to act as a standard thin AP with a connection back to the controller through at least one other AP, which acts as a mesh hop.

Remote Users and Temporary Teaching Environments

Remote APs are a cost-effective solution to provide secure and centrally managed wired and wireless connectivity to locations that only need a small number of APs. Remote APs can connect directly via Ethernet to a public/private Internet connection or to the LAN. Remote APs automatically discover the master controller, establish a secure VPN tunnel back to the data center and extend secure wired and wireless connectivity to a single remote user or a group of users. Application traffic can be tunneled back to the data center or bridged locally. For cases where more than one AP is needed at the remote site, additional APs can be connected to power sources and create a mesh connection back to the network-connected remote AP. The result is a wireless hotspot that can be set up on the fly without any Ethernet LAN cabling and without IT resources.

Virtual Intranet Agent

Dell's Virtual Intranet Access (VIA) agent provides automatic secure connectivity for Windows laptops. VIA automatically creates a secure connection back to the school network whenever needed, leveraging CIPA compliant network services such as web filters. Unlike traditional VPN software, VIA provides a zero-touch experience for the end user and can even configure the wireless LAN (WLAN) settings on laptops.

Multivendor Wired and Wireless Management

The AirWave Wireless Management Suite (AWMS) from Dell delivers operational efficiency for teams managing rapidly changing networks and supporting mobile users who connect via the wireless LAN as well as wired Ethernet ports.

As the only multi-vendor operations solution on the market that manages wired and wireless infrastructure as well as mobile devices, AirWave eliminates the need for multiple, disparate single-purpose management tools. Its easy-to-use interface and user-centric approach enables your service desk to triage connectivity issues while your valuable network engineering staff focuses on more strategic work. You also get a much simpler way to enforce policies, and actionable information that lets you plan for the future.

Applications and services running on backend

Dell's centralized network architecture enables network monitoring, control and troubleshooting to be performed from a single location regardless of whether the network spans a single school or across a school district. For schools that are part of a school district, a separation of duties may be mandated between IT managers at each school. Dell offers a "manager of managers" capability that logically separates the information available to each management user hierarchically. Dell's infrastructure provides remote packet capture so IT managers don't have to walk across campus or worse, drive somewhere, to troubleshoot problems. Additionally, Dell offers a full real-time view of the RF environment for each building that is part of the campus network. The network manager can perform all maintenance and upgrades centrally from one location, receiving alerts on intrusion or other security events as they happen.

More Efficient School Networks with Adaptive Radio Management

Adaptive Radio Management (ARM) is an RF management technology that allows every student or client to operate at its highest throughput, resulting in more efficient use of the spectrum, 20% better fairness, 40% less interference and more than 30% more overall throughput. Acting alone, Wi-Fi clients do not always work together cooperatively, or select the optimal band, channel, and access point. ARM solves these problems by using infrastructure-based controls that leverage information from PowerConnect-W centrally managed WLAN infrastructure to optimize client behavior: By automatically adjusting how Wi-Fi clients interact, ARM ensures that **data, voice, and video** applications have sufficient network resources, including airtime, to operate properly. By closing the gap between the theoretical performance of Wi-Fi clients and what is achieved in real-world deployments, ARM delivers a better wireless experience for students, teachers and staff.

Key ARM features include:

Band steering – actively guides faster 802.11a/n clients to the best available wireless channel. The result is better noise immunity, fewer sources of interference, and more available channels. If a client supports both 2.4GHz and higher speed 5GHz bands, this feature will automatically direct it to the 5GHz band for best performance

Spectrum load balancing – enables PowerConnect-W access points and Multi-Service Mobility Controllers to dynamically shift Wi-Fi clients to access points on channels with available bandwidth. This technique is intended to prevent degraded network performance due to over-subscription

Coordinated access – coordinates access to a wireless channel, across all access points that share that channel, to overcome the challenges of densely populated deployments such as lecture halls, airport lounges, and conference centers

Co-Channel Interference Mitigation – adjusts access point rate adaptation to control interference and shifts access points with excess capacity to air monitor mode

Airtime fairness – scheduled access for dense deployments delivers equal access to all Wi-Fi clients. This feature works with all 2.4GHz and 5GHz Wi-Fi clients, regardless of wireless chip manufacturer or standard operating system supplier

Performance protection – prevents higher speed clients using 802.11n from being compromised by slower 802.11b/g clients

Realizing the full potential of your K-12 Network

Before connected learning can take root in new teaching contexts, a secure and reliable, multimedia-grade Wi-Fi network that provides access, anywhere, anytime needs to be in place.

Dell's K-12 Wireless Networking solution provides the following benefits.

Scalability

The Adaptive Radio Management (ARM) greatly improves scalability of bandwidth intensive applications such as video in high-density classroom environments. Spectrum Load balancing improves scalability by spreading users or clients across available wireless spectrum

Mobility

PowerConnect-W securely delivers networks to students and teachers, wherever they work or roam with the industries only user-based state-full firewall.

Data, Voice and Multimedia Access

PowerConnect-W delivers a range of technologies that work on top of the IEEE 802.11n standard to deliver not just data but also high quality, uninterrupted video over a multi-use WLAN.

Key features are:

Video Optimized Over the Wire, PowerConnect-W optimizes video over the air between APs and clients by actively monitoring the client mix, network capacity, application usage across clients, RF characteristics, and video subscription requirements. Based on this real-time assessment of network conditions, the network is continuously optimized and client behavior managed to support high definition (HD), multi-channel video.

In addition, **Multicast Optimization** across the LAN is important because video can account for a large percentage of network bandwidth. PowerConnect-W controller receives multicast streams from video sources in the network core, and then uses IGMP snooping to determine the state of the client. Video is sent only to access points with active clients, preserving considerable wired network capacity, especially when high definition channels are in use.

Multimedia applications are stressed, even in a wired network. However, PowerConnect-W leverages a unique **Adaptive Radio Management (ARM)** technology, Quality of Service features, and policy enforcement mechanisms ensure that the signals get through. Thus, K-12 can deliver video wherever and whenever it needs without the burden of installing and maintaining an expensive cable plant.

Security

Security is often a primary concern of organizations contemplating the deployment of WLAN systems but today's wireless networks are actually more secure than the average wired Ethernet network - especially with PowerConnect-W. PowerConnect-W delivers industry leading security solutions that are without peer. Only PowerConnect-W integrates an ICSA certified stateful firewall capabilities, enabling role based access control and per application quality of service (QoS) policies, instead of VLAN and port level security and QoS. Only PowerConnect-W has centralized encryption to prevent eavesdropping on user data and malicious attacks on APs. Dell integrates advanced wireless IPS (WIPS) functions in order to improve security posture of a WLAN and prevent substantial cost of deploying a separate overlay WIPS solution. PowerConnect-W WLAN products are FIPS 140-2 and Common Criteria certified and are used in environments where security is of paramount concern, including military and government agencies around the world.

PowerConnect-W approach to network security is modeled after the best security practices widely used in the defense and intelligence sectors. Every user is treated as un-trusted entity until they prove themselves to be trustworthy and after that each users activities are monitored and usage rights are constantly enforced. This capability is achieved through a combination of centralized encryption and built-in firewall in the PowerConnect-W controller.

PowerConnect-W identity-based security solution dramatically improves network security by eliminating excess privilege on the network while also providing identity-based auditing of activity. Traditional fixed networks can only apply access rights to ports or VLANs. Mobile users and devices, by definition, do not connect to the network through a fixed port. The network must therefore identify every user and device that joins the network. Once this identity is known, custom security policies may be applied to the network so that only access appropriate to the business needs of the user or device is provided.

Reliability

PowerConnect-W Adaptive Radio Management (ARM) allows mixed 802.11a, b, g, and n client types to interoperate at the highest performance levels, RF airtime to be allocated fairly, and co-channel and adjacent channel interference to be mitigated. PowerConnect-W ARM does not require any proprietary client software – which can be problematic, as it requires vigilant revision control and may not be available for all operating systems or compatible with all client hardware. ARM ensures low-latency roaming, consistently high performance, and maximum client compatibility in a multi-channel environment. Unlike proprietary single-channel architectures, ARM is designed to enable maximum efficiency and performance across the access points (AP) deployed without compromising interference mitigation, scalability, or interoperability – common problems of single-channel architectures.

Management

In addition, the PowerConnect-W is designed to install as easily as possible. Some other vendors require changes to the wired network to be able to deploy their AP. PowerConnect-W acts as a pure overlay, for plug-n-play ease.

PowerConnect-W, AirWave Network Management is a powerful, purpose-built software platform that is designed to scale to manage the largest district networks. It provides a comprehensive management solution for wired and wireless network. It's easy to use and deploy and it can generate a report or identify a security issue

PowerConnect-W VisualRF gives K-12 IT an accurate view of the entire network without ever leaving the desk. It automatically generates a map of the K-12 RF environment and the underlying wired topology, showing what the network looks like — in real time. VisualRF builds this map using RF measurements gathered from active wireless access points and controllers, without requiring K-12 to buy a costly, separate location appliance.

Multiple (<200) PowerConnect controllers and APs (<3000) can be managed through a single "master controller" user interface. PowerConnect-W does not mandate the use of a separate appliance for basic functionality such as RF visualization, location tracking, or multi-controller management, all of which are capabilities that are built into the designated master controller. Consequently, for extensive historical data storage, monitoring and reporting, PowerConnect-W's AirWave Wireless Management Suite (AWMS) delivers a single, easy-to-use console that gives the entire IT staff full visibility and control over their wireless network. It enables management support for WiFi, Mesh, WiMAX and point-to-point wireless equipment from seventeen different vendors. AWMS significantly reduces operating costs through its intuitive user interface, effective diagnostic tools, virtualized admin access, automated compliance audits, etc.

Cost

The key efficiency for Dell's K12 WLANs is that the PowerConnect-W does not require a 1:1 ratio of ports to devices, as would be the case with a wired network.. This flexibility makes it much more affordable to deliver current and future connectivity in your school allowing students and staff access to their education services from anywhere on your school campus without being disconnected. Comparing the cost of PowerConnect-W to any of its competitors presents a tremendous saving without compromising features.

Conclusion

This K-12 wireless network-planning guide has outlined requirements and proposed solutions to build a dynamic, secured and cost effective Wireless LAN infrastructure. The paper articulates WLAN infrastructure as part of the foundation infrastructure to enable connected classrooms for K-12 environments. The applications and services that utilize and run in a K-12 WLAN environment play a major role in facilitating interactive learning and collaboration while at the same time allowing the teacher to track progress in real-time as students engage with their digital learning community.

The majority of next generation smart devices and connected classroom hardware comes with Ethernet WLAN connections built-in. This, along with the need for mobility, makes WLAN the primary network choice for K-12 environments. PowerConnect-W leveraging 802.11n provides outstanding performance and easily supports concurrent bandwidth intensive multi-media applications, while guaranteeing a high level of service.